UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/522,472	02/06/2006	Jan Camenisch	CH920020013US1	3674

68168 7590 07/08/2009

MICHAEL BUCHENHORNER, P.A.
8540 SW 83 STREET
SUITE 100
MIAMI, FL 33143

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
07/08/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

michael@buchenhorner.com
ana@buchenhorner.com
AnaBuch@gmail.com

Office Action Summary	Application No.	Applicant(s)	
	10/522,472	CAMENISCH ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-14,16-20 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7, 9-14, 16-20, and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to Amendment filed 3/16/2009. Claims 1, 4, 7, 12 16-20 and 22 are amended. Claim 8, 15 and 21 is cancelled. Claims 1-7, 9-14, 16-19 and 21 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-3, 9-12, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schweitzer et al. (US Patent No. 5,850,450 and Schweitzer hereinafter) in view of Hopkins and further in view of Kocher et al. (US Patent No. 6,304,658 and Kocher hereinafter).

3. As to claim 1, Schweitzer teaches a method comprising providing a secret cryptographic key and a public cryptographic key applicable in a network of connected computer nodes using a signature scheme (i.e., ...teaches generating a two-key encryption key set comprising a private component and a public component [claim 5]),

the method being executable by a first computer node and the step of providing comprising the steps of: - generating the secret cryptographic key by - selecting two

random factor values (i.e., ...teaches generating a first random prime number; generating a second random prime number [claim 5]), - multiplying the two selected random factor values to obtain a modulus value (i.e., ...teaches producing a modulus by multiplying said first random number by said second random prime number [claim 5]), and - selecting a secret base value (i.e., prime number) as a function of the modulus value, wherein the secret base value forms part of the secret cryptographic key (i.e., ...teaches generating a first and second key based on said first and second prime numbers [claim 8]);

- deleting the two random factor values (i.e., ...teaches first and second random prime numbers is obtained by concatenating a first and second plurality of random bytes, respectively, and further wherein the contents of said random bytes are associated with a random event the use of random number [claim 5]. Examiner contends the fact that the numbers are random inherently teaches they will be deleted automatically);

sending the message to a second computer node within the network for verification (e.g., authenticity) (col. 15, lines 35-45).

Schweitzer does not teach:

- providing the public cryptographic key within the network; - generating the public cryptographic key by

- selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value, wherein the public base value and the

modulus value form part of the public cryptographic key using the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value on a message.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schweitzer as introduced by Hopkins. Hopkins discloses:

providing the public cryptographic key within the network (to provide the cryptographic key within the network [fig. 1]);

generating the public cryptographic key by - selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value, wherein the public base value and the modulus value form part of the public cryptographic key (for the purpose of generating a cryptographic key Hopkins provides for the an associated individual modulus n.sub.i that is a number formed as a product of one or more of the k prime factors of the group modulus n such that an associated individual private exponent d.sub.i is determined based on a selected public group exponent e, and also based on the prime factors of the associated individual modulus n.sub.i. Hopkins further provide for each of the individual private exponents

may be determined as a number congruent to the inverse of the public group exponent e, modulo the Euler Totient function of the associated individual modulus n.sub.i [par. 18]),

using the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value on a message (for purpose of verifying a signature value Hopkins provides to verify the signed message M would of course need to know the public key including modulus n and the public exponent e in order to compute h(M)'.. [par. 57]).

Therefore, given the teachings of Hopkins, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schweitzer by employing the well known features of using a public key and exponent values to verifying a signature value of a message disclosed above by Hopkins, for which signature security will be enhanced [par. 57]).

The combination of Schweitzer and Hopkins does not teach:

If the public cryptographic key has been revoked abort signing of the message. However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schweitzer and Hopkins as introduced by Kocher. Kocher discloses:

If the public cryptographic key has been revoked (e.g., secret key leaked) abort signing of the message (to provide the means to invalidate associated key data in instances were the secret key data has been leaked [abstract]. Those skilled in the art would recognize by invalidating associated key material (e.g., public key), message signing using associated key material (e.g., public key) would thereby not be allowed

(i.e., message signed with an invalid public key cannot be validated during authentication). Note: Applicant describes in paragraph 64 the abort process occurs when the secret cryptographic key associated to the public key is leaked).

Therefore, given the teachings of Kocher, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schweitzer and Hopkins by employing the well known feature of rendering invalid (e.g., aborting) key material associated to previously leaked secret key data (e.g., associated public key) as disclosed above by Kocher, for which signature verification will be enhanced [abstract].

4. As to claim 2, Schweitzer teaches a method further comprising providing a description of the exponent values within the network (i.e., ...teaches D is the private exponent and E is the public exponent, then the "encryption" key set comprises [E;N], whereas the "decryption" key set comprises [D;N]. The host 10 can send an encrypted message to the electronic data module 100 (shown in FIG. 1) having the decryption key, D, stored internally thereto, by computing M.sup.E Mod N, where M denotes the plaintext. The data module 100, upon receiving the cipher text, C, can decrypt by computing C.sup.D Mod N using the stored decryption key, D [col. 15, lines 20-35]).

5. As to claim 3 and 9, the system disclose by Schweitzer teaches substantial features of the claim invention (discussed above) it fails to disclose:

A method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in the event of a detected intrusion (claim 3).

A method further comprising applying each of the exponent values to at most one signature value (claim 9).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schweitzer as introduced by Hopkins. Hopkins discloses:

A method further comprising defining an order of the selected exponent values for enabling to communicate the validity of the signature value in the event of a detected intrusion (claim 3) (to define a exponent order for purpose of signature verification [par. 57]).

A method further comprising applying each of the exponent values to at most one signature value (claim 9) (to apply an exponent value for verification of a signature [par. 57]).

Therefore, given the teachings of Hopkins, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schweitzer by employing the well known features of using exponent values to verifying a signature value of a message disclosed above by Hopkins, for which signature security will be enhanced [par. 57].

6. As to claim 10, Schweitzer teaches a computer program (i.e., processor instruction performed by processor) element comprising program code means for performing the method of claim 1 when said program is run on a computer [20, fig. 1].

7. As to claim 11, Schweitzer teaches a computer program product stored (i.e., processor instructions) on a computer usable medium, comprising computer readable program means for causing a computer to perform the method according to claim 1 [20, fig. 1].

8. As to claim 12, Schweitzer teaches a network device comprising: a computer program product for causing a computer to perform a method comprising of;

generating the secret cryptographic key by (i.e., ...teaches generating a two-key encryption key set comprising a private component and a public component [claim 5]):

selecting two random factor values (i.e., ...teaches generating a first random prime number; generating a second random prime number [claim 5]),

multiplying the two selected random factor values to obtain a modulus value (i.e., ...teaches producing a modulus by multiplying said first random number by said second random prime number [claim 5]);

and selecting a secret base value (e.g., prime number) as a function of the modulus value, wherein the secret base value forms part of the secret cryptographic key

(i.e., ...teaches generating a first and second key based on said first and second prime numbers [claim 8]);

deleting the two random factor values (i.e., ...teaches first and second random prime numbers is obtained by concatenating a first and second plurality of random bytes, respectively, and further wherein the contents of said random bytes are associated with a random event the use of random number [claim 5]. Examiner contends the fact that the numbers are random inherently teaches they will be deleted automatically);

sending the message to a second computer node within the network for verification (e.g., authenticity) (col. 15, lines 35-45);

and a processor for executing the method, the processor having access to exchanged messages in the network [20, fig. 1].

Schweitzer does not teach:

- generating the public cryptographic key by selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value, wherein the public base value and the modulus value form part of the public cryptographic key using the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value on a message;

and providing the public cryptographic key within the network.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Schweitzer as introduced by Hopkins. Hopkins discloses:

generating the public cryptographic key by selecting a number of exponent values, and deriving a public base value from the exponent values and the secret base value, wherein the public base value and the modulus value form part of the public cryptographic key (for the purpose of generating a cryptographic key Hopkins provides for the an associated individual modulus n.sub.i that is a number formed as a product of one or more of the k prime factors of the group modulus n such that an associated individual private exponent d.sub.i is determined based on a selected public group exponent e, and also based on the prime factors of the associated individual modulus n.sub.i. Hopkins further shows that each of the individual private exponents may be determined as a number congruent to the inverse of the public group exponent e, modulo the Euler Totient function of the associated individual modulus n.sub.i [par. 18]),

using the public cryptographic key and at least one of the selected exponent values is usable for verifying a signature value on a message; (for purpose of verifying a signature value Hopkins provides to verify the signed message M would of course need to know the public key including modulus n and the public exponent e in order to compute h(M)'.. [par. 57]);

and providing the public cryptographic key within the network (to provide the cryptographic key within the network [fig. 1]).

Therefore, given the teachings of Hopkins, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Schweitzer by employing the well known features of using a public key and exponent values to verifying a signature value of a message disclosed above by Hopkins, for which signature security will be enhanced [par. 57].

The combination of Schweitzer and Hopkins does not teach:

If the public cryptographic key has been revoked abort signing of the message.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schweitzer and Hopkins as introduced by Kocher. Kocher discloses:

If the public cryptographic key has been revoked (e.g., secret key leaked) abort signing of the message (to provide the means to invalidate associated key data in instances were the secret key data has been leaked [abstract]. Those skilled in the art would recognize by invalidating associated key material (e.g., public key), message signing using associated key material (e.g., public key) would thereby not be allowed (i.e., message signed with a invalid public key cannot be validated during

authentication).Note: Applicant describes in paragraph 64 the abort process occurs when the secret cryptographic key associated to the public key is leaked).

Therefore, given the teachings of Kocher, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Schweitzer and Hopkins by employing the well known feature of rendering invalid (e.g., aborting) key material associated to previously leaked secret key data (e.g., associated public key) as disclosed above by Kocher, for which signature verification will be enhanced [abstract].

9. As to claim 22, Schweitzer teaches a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing functions of a network device [20, fig. 1], the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 12 [20, fig. 1].

10. Claims 4-7, 13, 14, and 16 -20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hopkins in view of Kocher.

11. As to claim 4, Hopkins teaches a method comprising providing a signature value on a message in a network of connected computer nodes (i.e., ... teaches distributing individual private keys to a plurality of authorized individuals each of whom may then

sign a message using his or her associated individual private key to create an associated partial digital signature [par. 30]), the method being executable by a first computer node and the step of providing comprising the steps of:

- selecting a first signature element (i.e., prime factor) from a plurality of signature elements (e.g., a collective group of prime factors) comprising said signature (e.g., signing a message) (i.e., ... teaches a signing process using the group private key D wherein each of the members of each group has control over at least one of the prime factors p.sub.1, p.sub.2,... p.sub.k, and wherein each group of individuals collectively has control of all of the prime factors p.sub.1, p.sub.2,.., p.sub.k, but wherein no single one of the individuals of the group controls all of the prime factors used by the entity [par. 67]);

- selecting a signature exponent value from a number of exponent values, said signature comprised of a plurality of signature exponent values (i.e., ...teaches an associated individual private exponent d.sub.i that is determined based on a selected public group exponent e [claim 3]);

and - deriving a second signature element from a provided secret cryptographic key (i.e., ... teaches deriving a hash value of the message to be signed and then performing a mathematical operation on that value using the private key [par. 9]), the message, and the number of exponent values such that the first signature element, the second signature element and the signature exponent value satisfy a known relationship with the message and a provided public cryptographic key (i.e., ...teaches messages associated with an entity represented by the group, and the prime numbers

p.sub.1, p.sub.2,.., p.sub.k are referred to as factors of the group modulus n. As mentioned, the prime numbers p.sub.1, p.sub.2... p.sub.k satisfy the criteria of being distinct, random, and suitable in accordance with relationships (2) through (6), above. The private key D, defined in accordance with relationship (7) above, which includes the composite number n and the private exponent d [par. 66]),

wherein the signature value comprises the first signature element, the second signature element, and a signature reference to the signature exponent value (i.e., ... teaches sub-tasks are then solved to determine results S.sub.1, S.sub.2... S.sub.z which are subsequently combined in accordance with a combining process to produce the signature S [par. 59] ... further teaches digital signatures are generated by each individual at a corresponding one of the individual systems 16 (FIG. 1) based on the associated individual cryptosystem defined by the associated individual modulus n.sub.IND and the associated individual private key exponent d.sub.IND [par. 78]), the signature value being sendable within the network to a second computer node for verification (i.e., ...teaches the digital signature is attached to the corresponding message and transmitted to a second party [par. 9]).

Hopkins does not teach:

If the public cryptographic key has been revoked abort signing of the message.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Hopkins as introduced by Kocher. Kocher discloses:

If the public cryptographic key has been revoked (e.g., secret key leaked) abort signing of the message (to provide the means to invalidate associated key data in instances were the secret key data has been leaked [abstract] Those skilled in the art would recognize by invalidating associated key material (e.g., public key), message signing using associated key material (e.g., public key) would thereby not be allowed (i.e., message signed with a invalid public key cannot be validated during authentication).Note: Applicant describes in paragraph 64 the abort process occurs when the secret cryptographic key associated to the public key is leaked).

Therefore, given the teachings of Kocher, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hopkins by employing the well known feature of rendering invalid (e.g., aborting) key material associated to previously leaked secret key data (e.g., associated public key) as disclosed above by Kocher, for which signature verification will be enhanced [abstract].

12. As to claim 5, Hopkins teaches a method where the step of deriving a second signature element further comprises deriving a signature base value using a provided public cryptographic key, the provided secret cryptographic key, and the exponent values (i.e., ...teaches digital signatures are generated by each individual at a

corresponding one of the individual systems 16 (FIG. 1) based on the associated individual cryptosystem defined by the associated individual modulus n.sub.IND and the associated individual private key exponent d.sub.IND [par. 78]).

13. As to claim 6, Hopkins teaches a method further comprising deriving a previously presented secret cryptographic key from the provided secret cryptographic key and the selected signature exponent value (i.e., ... teaches the first individual private key includes: an associated individual modulus n.sub.1 that is determined as the product of a number m.sub.1 of distinct prime factors of the group modulus n; and an associated individual private exponent d.sub.1 that is determined based on a selected public key exponent e and based on the m.sub.1 prime factors of the associated individual modulus in accordance with 1 d 1 e - 1 mod (j m 1 (p j 1) [par. 19]).

14. As to claim 7, Hopkins teaches a method comprising verifying a signature value on a message in a network of connected computer nodes (i.e., ... teaches a verifying a signature on a message [par. 94]), the method being executable by a second computer node and the step of verifying comprising the steps of:

- receiving the signature value from a first computer node the digital signature is attached to the corresponding message and transmitted to a second party. Verification of the digital signature is accomplished by computing a new hash result of the original message using the same hash function that was used to create the digital signature. Using the public key to invert the received signature [par. 9]);

- deriving a signature exponent value from the signature value (i.e., ...teaches A verification process of the Multi-Prime signature scheme provides for converting the signature S to a candidate hash h(M)' using the public exponent e as a verification exponent [par. 56]);

and - verifying whether the signature exponent value and part of the signature value satisfy a known relationship with the message and a provided public cryptographic key (i.e., ...teaches to verify the signed message M would of course need to know the public key including modulus n and the public exponent e in order to compute h(M)'. After computing h(M)', if it is determined that h(M)=h(M)', the signature would be verified as originating from the entity associated with the public exponent e and the modulus n [par. 57]), wherein the signature value was generated from a first signature element, a number of exponent values, a provided secret cryptographic key, and the message (par. 57).

Hopkins does not teach:

otherwise refusing the signature value,

If the public cryptographic key has been revoked abort signing of the message.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Hopkins as introduced by Kocher. Kocher discloses:

otherwise refusing (e.g., invalidate) the signature value (to provide signature invalidation capability [abstract]. Those skilled in the art would recognize once key material has been leaked, it is common to refuse (e.g., invalidate) all signatures signed using the public key).

If the public cryptographic key has been revoked (e.g., secret key leaked) abort signing of the message (to provide the means to invalidate associated key data in instances were the secret key data has been leaked [abstract]. Those skilled in the art would recognize by invalidating associated key material (e.g., public key), message signing using associated key material (e.g., public key) would thereby not be allowed (i.e., message signed with an invalid public key cannot be validated during authentication). Note: Applicant describes in paragraph 64 the abort process occurs when the secret cryptographic key associated to the public key is leaked).

Therefore, given the teachings of Kocher, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hopkins by employing the well known feature of rendering invalid (e.g., aborting) key material associated to previously leaked secret key data (e.g., associated public key) as disclosed above by Kocher, for which signature verification will be enhanced [abstract].

15. Claims 8, (cancelled).

16. As to claim 13, Hopkins teaches a method further comprising applying each of the exponent values to at most one signature value [par. 57].

17. As to claim 14, Hopkins teaches a method further comprising applying each of the exponent values to at most one signature value [par. 57].

18. Claim 15, (cancelled).

19. As to claim 16, Hopkins teaches a computer program element comprising program code means for performing the method of claim 4, when said program is run on a computer [par. 39].

20. As to claim 17, Hopkins teaches a computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 4 [par. 39].

21. As to claim 18, Hopkins teaches a computer program element comprising program code means for performing the method of claim 7, when said program is run on a computer [par. 39].

22. As to claim 19, Hopkins teaches a computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 7 [par. 39].

23. As to claim 20, Hopkins teaches computer program element comprising program code means for performing the method of claim 8, when said program is run on a computer [par. 39].

24. Claim 21, (cancelled).

Response to Arguments

Applicant's Remarks 102 rejection

The Examiner contends applicant's arguments with regards to claims 4-6, 13, 16, and 17 are moot under the new 103 of Hopkins in view of Kocher. Kocher provides for the ability to invalidate key material (e.g., public key) associated with previously leaked secret key data. Those skilled in the art would recognize by invalidating associated key material (e.g., public key), message signing using associated key material (e.g., public key) would thereby not be allowed (i.e., message signed with an invalid public key cannot be validated during authentication).

The Examiner contends that the Examiner's argument stated above for claims 4-6, 13, 16 and 17 holds for claims 7, 14, 18 and 19 on the basis that Hopkins teachings has been modified by the teachings of Kocher. Claims 7, 14, 18, and 19 were

previously rejected solely under the teaching of Hopkins as presented in Office Action dated 12/15/2008; claims 7, 14, 18 and 19 now stand rejected under Hopkins in view of Kocher. Applicant's arguments with respect to claims 7, 14, 18, and 19 are moot under the new grounds of rejection.

Applicant's Remarks 103 rejection

The Examiner contends applicant's argument with regards to claim 1-2, 9-12, and 22 are moot under new grounds of rejection. The Examiner contends modifying the teaching of Schweitzer in view of Hopkins provides the ability to invalidate associated key material data (e.g., public key) when secret key data has been previously leaked. Those skilled in the art would recognize by invalidating associated key material (e.g., public key), message signing using associated key material (e.g., public key) would thereby not be allowed (i.e., message signed with an invalid public key cannot be validated during authentication).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431